Department of Defense

Critical Infrastructure Protection

2002 Executive Report





Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2002		**00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Department of Defense Critical Infrastructure Protection. 2002 Executive Report	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense,Washington,DC,20301**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**25**	

Department of Defense

Critical Infrastructure Protection

2002 Executive Report

2002

Critical Infrastructure Protection

Table of Contents

2002

Critical Infrastructure Protection

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

Letter from the Director, Critical Infrastructure Protection

Since September 11, 2001, the Nation and the Department of Defense (DoD) have had to come to terms with the possibility of fighting a war on U.S. soil for the first time in 60 years. The concept of attacking and protecting infrastructure assets critical to a nation's warfighting capabilities is as timeless as war itself. History is full of examples of smaller forces defeating larger forces when the smaller force correctly identified and attacked a critical vulnerability in the larger force's warfighting capability. Today, most people recognize that the United States' military is heavily dependent on a limited number of military and commercial infrastructure assets.

From its inception in 1998, the success of the DoD Critical Infrastructure Protection (CIP) Program has relied on the leadership of the Joint Staff, the vigilance of the uniformed services, the dedication of the DoD workforce to recognize infrastructure vulnerabilities, and the ability of our nation's first responders to manage of the consequences of enemy attack. The result of an effective Critical Infrastructure Protection (CIP) program has been the improved mission assurance of the DoD to function under adverse and even extreme conditions. The rise of a credible terrorist threat with potential access to weapons of mass destruction has heightened the DoD's need to improve analysis and assessment capabilities essential to ensure we adequately protect the infrastructure assets critical to our National Military Strategy. The bitter lesson of September 11, 2001, and the simultaneous Anthrax attacks on our nation has shown that law enforcement agencies alone can not protect our vital assets. Therefore we need to understand what assets are critical to mission success, reduce or eliminate related vulnerabilities, and understand the interdependencies that support our defense infrastructure. The DoD CIP vision is to assure that the critical infrastructure assets on which the DoD depends are always available to mobilize, deploy, and sustain military operations.

The work being done within the DoD CIP community represents the finest example of cooperation and collaboration between the DoD, Federal agencies, State and Local government, industry and national law enforcement since WWII. The enclosed Executive Summary provides a sample of the outstanding efforts and accomplishments of the DoD CIP community since September 11, 2001.

Thomas E. Bozek
Director
Critical Infrastructure Protection

2002

Critical Infrastructure Protection

Introduction

The Defense Infrastructure represents a complex and decentralized network of personnel, processes, systems, services, facilities, and equipment. Through functional sectors, the network provides the operational and technical capabilities essential to mobilizing, deploying, and sustaining military operations in peacetime and in war. The Department of Defense (DoD), other U.S. Government agencies, domestic and foreign private sectors, host-nation governments, third-nation governments, and multinational consortiums own or control these assets.

"It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible."

President George W. Bush
Executive Order on Critical Infrastructure Protection, issued 16 October 2001

The Defense Infrastructure crosses organizational and political boundaries. As DoD infrastructure and assets become more complex and interdependent with, at the same time, an increase in outsourcing and privatization, DoD readiness is affected in more ways than one. Advances in information technology and the need for higher efficiency may increasingly automate and link infrastructures, but they also create new vulnerabilities. These run the gamut from equipment failure to human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will require flexible, evolutionary approaches that span both public and private sectors and protect both domestic and international security.

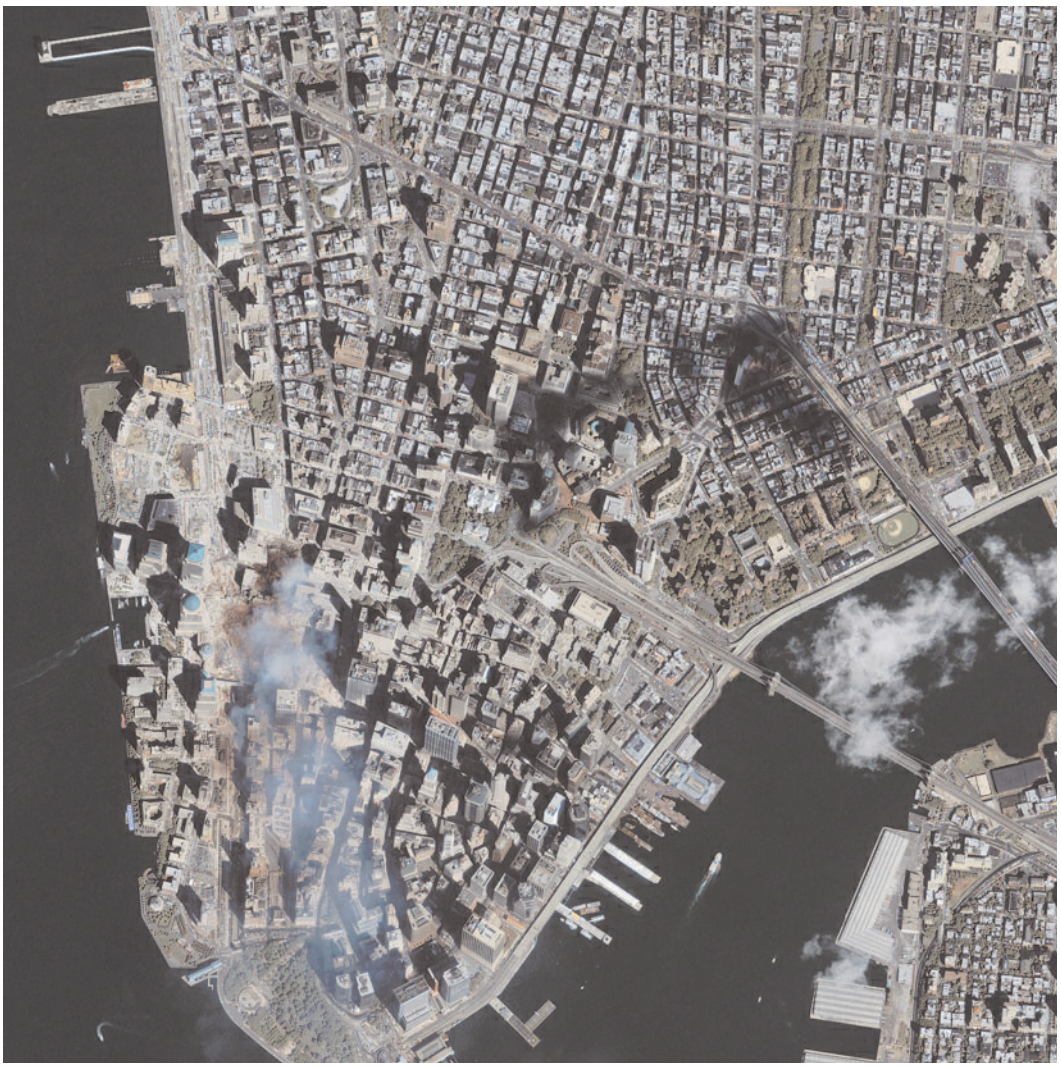
The terrorist attacks of 11 September 2002 made painfully clear the damage that a determined adversary can inflict. In the wake of these horrific events, it is impossible to ignore the vulnerability of infrastructure assets critical to the political, economic, and security interests of the United States.

Since 1986, the Department of Defense has undergone a deep transformation, moving away from the major conventional land warfare posture of the Cold War toward more flexibility and responsiveness to the growing threat of asymmetric warfare. The United States is no longer subject to attack only by conventional military forces. Increasingly,

smaller groups of terrorists or even a determined lone hacker breaking into essential systems can cause major damage.

"Our challenge in the 21st century is to defend our cities and our infrastructure from new forms of attack while projecting force over long distances to fight new and perhaps distant adversaries."

Secretary of Defense Donald H. Rumsfeld,
31 January 2002



Manhattan, New York—September 15, 2001. Photo courtesy of Space Imaging.

The Foundation for Critical Infrastructure Protection in the Department of Defense

The need to protect critical infrastructure is recognized at the highest levels of the National Command Authority. The President of the United States, the Secretary of Defense, and the Chairman of the Joint Chiefs of Staff have all published detailed guidance requiring the Defense community to establish effective programs for such a protection. But even without directives requiring formal CIP programs, protecting critical

Executive Order 13010, "Critical Infrastructure Protection" (July1996), established the President's CIP Commission and supporting structure, with the purpose of protecting information systems for critical infrastructure—including emergency preparedness communications—and the physical assets that support such systems.

Presidential Decision Directive 63, "Critical Infrastructure Protection" (May 1998), was issued in recognition of fundamental changes in the primary threats to the security of the United States. It recognized the "growing potential vulnerability" of "physical and cyber-based systems essential to the minimum operations of the economy and government." The directive established a "national goal" to institute a comprehensive program to identify critical infrastructures (public and private), assess their vulnerability, and mitigate the risk to those infrastructures.

Executive Order 13228, "Establishing the Office of Homeland Security and the Homeland Security Council" (October 2001), charged this Office and Council with the mission to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States.

Department of Defense Directive 5160.54, "Critical Asset Assurance Program" (January 1998), established policies and assigned responsibilities "for the protection and assurance of DoD and non-DoD Critical Assets worldwide."

The **2001 Quadrennial Defense Review (QDR)** recognized CIP as one of six critical operational goals that provide the focus for DoD's transformation efforts.

The **Department of Defense Contingency Planning Guidance (CPG)** establishes goals to "identify, prioritize, and assess the availability of those cyber and physical capabilities and infrastructures, both foreign and domestic, which are essential to successful execution of plans." The CPG directs coordinated planning with U.S. Government agencies, and with host nations and their infrastructure providers to assure availability of national and international infrastructure essential to national defense and global force projection and sustainment.

assets is an obvious fundamental requirement for all defense activities. In conventional wars, critical assets have always been considered lucrative targets. They become even more so in an asymmetric conflict where small unconventional forces seek to inflict maximum damage with minimal resources.

The Department of Defense Critical Infrastructure Protection Program

Critical Infrastructure Protection (CIP) is a Department of Defense program intended to minimize the consequences of any potential or successful threat to a government or private-sector infrastructure. The CIP process involves four successive steps:

1. Identifying infrastructure assets critical to DoD's warfighting mission
2. Assessing vulnerabilities for each critical infrastructure
3. Developing remediation plans, mitigation strategies, and tactical work-arounds to deal with damaged, destroyed, or inaccessible infrastructures
4. Integrating these various plans into DoD deliberate and crisis planning documents

The Department of Defense CIP Concept

Behind the concept of Critical Infrastructure Protection is mission assurance. This means that the program ensures that U.S. military operations can take place. As described above, the program identifies, assesses, and assures cyber and physical assets essential to these operations. Because vulnerabilities in interdependencies between assets and infrastructure represent targets of opportunity for an adversary, it also stresses the utmost importance of understanding these interdependencies .

The Department of Defense CIP Vision

Naturally following is the DoD CIP vision, which is to ensure that the critical infrastructure assets on which DoD depends are always available to mobilize, deploy, and sustain military operations. This vision creates dependable and trustworthy cyber and physical infrastructures. By reducing the number of single points of failure, CIP denies advantages to adversaries. It creates real-time situational awareness—supported by modeling and simulation—which will enable Combatant Commanders to adjust operations in anticipation of adverse infrastructure events. Modeling and simulation reliably describe

the unfolding operational environment. The process is close enough to allow accurate predictions of the operational environment and time for making needed changes and adjustments to military operations.

The Department of Defense CIP Mission

The work of the Office of the Assistant Secretary of Defense (OASD) for Command, Control, Communications, and Intelligence (C3I) enables the military forces of the United States to generate, use, and share the information needed not only to survive but to succeed on every mission. By building the foundation for network operations, OASD(C3I) provides leadership for the conversion of the Department of Defense to the Information Age.

The Department of Defense CIP Strategy

The DoD CIP strategy focuses on support to the warfighter and aligns with the Combatant Commander's requirements and priorities, DoD core business processes, and the United States Code Title X and Code of Federal Regulations Title 32 responsibilities of the Services and Defense agencies.

The DoD CIP strategy is built upon nine core activities:

- **CIP Awareness** - The success of the DoD CIP Program depends largely first on leadership, and then on creating in the workforce an awareness of the Department's dependence on critical and potentially vulnerable infrastructure assets.
- **Analysis and Assessment** - Mission analysis and infrastructure assessment are key to the DoD CIP Program. The purpose of analysis and assessment is to:
  - Determine what assets are truly critical to specific missions, including identification of support infrastructure assets and their dependency on other assets
  - Identify vulnerabilities that could result in degradation or disruption of missions, regardless of the cause
  - Assess the consequences of cascading failures on operations, and identify possible corrective actions
- **Indications and Warning** - CIP indications and warning identifies requirements, capabilities, and essential elements of information required to ensure the timely receipt and coordination of information related to potential critical infrastructure disruptions and their impact on defense operations. CIP indications and warning capabilities must embrace and expand beyond the current focus on intelligence information regarding potential enemy threats.
- **Consequence Management** - The present monitoring analysis capability for the cyber and physical infrastructure is manual, making it ineffective and time-con-

suming. Where practical, the analysis capability must be automated. Future characterization efforts will include the identification, instrumentation, visualization, and monitoring of infrastructure performance. Future characterization will also provide a more focused definition of the roles and responsibilities of the Defense Special Function Lead Components and guidance for developing Special Function Support Plans.

- **Investment Strategy -** To date DoD CIP has relied on two major supplemental funding increments, the fiscal year (FY) 1999 Supplemental and the FY 2002 Defense Emergency Response Fund (DERF), as well as the consistent support of the Joint Program Office - Special Technical Countermeasures (JPO-STC) to sustain the CIP program. In addition, The DoD CIP Directorate has coordinated with the services to establish program element codes to fund Service CIP efforts. Ultimately the CIP Program must have a stable financial baseline to ensure the DoD's mission assurance capability.
- **Research and Development (R&D) Strategy** - The DoD CIP Program recognizes the need (1) to develop, manage, and coordinate R&D requirements and activities across the DoD, (2) to develop an integrated and coherent effort that complements and leverages ongoing DoD R&D and (3) to address the CIP needs of the warfighter and the DoD CIP community.
- **CIP Outreach, Education, and Training** - One of the goals of the DoD CIP Program is to provide defense leaders at all levels with a better appreciation of their reliance on critical infrastructure assets, the interdependencies among these critical assets, and the consequences of their failure. Having this appreciation will enable these leaders to integrate CIP into existing plans and to forge working partnerships with state and local governments and off-base infrastructure providers to ensure that vulnerabilities are identified and corrected or mitigated.
- **National-Level Interface** - The DoD CIP strategy recognizes the need to develop operational relationships with other Federal departments and agencies because of the Department's dependence on non-DoD organizations, assets, and infrastructures. This effort will ensure that the evolution of the DoD CIP strategy is consistent with the national CIP effort and fully supports it.
- **Defense Industrial Base** - The Defense Industrial Base (DIB) comprises DoD product and service providers. Many services and products are essential to mobilize, deploy, and sustain military operations; therefore, they constitute critical assets for the DoD. The OASD(C3I) works with the Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics [OUSD(AT&L)] to establish the DIB as a DoD infrastructure sector and to assign OSD responsibility for a DIB Special Function Coordinator. DoD will seek a collaborative partnership with the DIB on CIP matters.

The Department of Defense Critical Infrastructure Protection Program Organization

CIAO Council

The ASD(C3I)—or the DoD Critical Infrastructure Assurance Officer (CIAO)—sits on the National Critical Infrastructure Assurance Council and chairs the DoD Chief Infrastructure Assurance Officer Council. Composed of the Military Service CIAOs and DoD sector leads, the Council provides executive oversight for the implementation of the DoD CIP Plan and advice to the ASD(C3I) regarding responsibilities as CIAO, Chief Information Officer (CIO), and CIP Functional Coordinator for National Defense.

CIP Integration Staff

The CIP Integration Staff (CIPIS) is a working group chaired by the staff of the ASD(C3I) and composed of leads from each sector and Service. The CIPIS developed and implements the DoD CIP Execution Plan, a plan of action, with milestones for implementing the DoD CIP Program.
Since its formation in 1999, the CIP Integration Staff has become the center for debate and action on critical cyber and physical issues facing the Department's multiple interests.

CIPIS Mission: *Plan, coordinate, and integrate the DoD Critical Infrastructure Protection (CIP) program using a total risk-based management approach to enhance the operational readiness and availability of DoD assets and infrastructures for use by the warfighters and supporting elements*

The CIPIS participation has now grown to encompass more than 40 leading agencies, including combat support agencies (such as the Defense Threat Reduction Agency, the National Imagery and Mapping Agency, the National Security Agency, the Defense Logistics Agency, the Defense Information Systems Agency, and the Defense Intelligence Agency), Defense Industrial Base representatives (such as the National Defense Industrial Association), communications industry leaders (such as the National Communications System and the National Security Telecommunications Advisory Committee), and the Military Departments.

The mission of this unprecedented coalition is to significantly improve DoD's operational capability and readiness by fully integrating all DoD CIP efforts. The CIPIS is moving the DoD CIP Program forward by accelerating the adoption of critical infrastructure protection practices, technologies, policies, education, and standards. Other

valuable functions of the CIPIS are to establish a link between DoD and non-DoD government agencies and to bring industry and government together in the interest of critical infrastructure protection. The CIPIS has formed relationships and accomplished projects with key Federal agencies, including the Department of Commerce and the National Institute of Science and Technology (NIST).

CIPIS members have access to a clearinghouse of the best CIP-related information possible on emerging trends, policies, and products, including databases, pilot projects, studies, staff papers, directories, and other resources. With the receipt of the FY 2002 Defense Emergency Response Funding, the CIPIS members have come together to support U.S. Pacific Command (USPACOM) efforts to design a CIP appendix to a standing operational plan (OPLAN) as the first operational application of the CIP analytical methodology.

The Department of Defense CIP Directorate

The mission of the CIP Directorate is to establish and maintain a comprehensive DoD-wide, fully integrated, and sustainable program, that ensures that DoD and national and international infrastructures critical to National Security remain viable in times of peace, crisis, and war. This includes networking infrastructures essential to planning, mobilizing, deploying, and sustaining military operations, as well as those needed for a smooth transition to post-conflict operations. The CIP Directorate sets DoD CIP policy, coordinates the monthly CIPIS meetings, sets the agenda for the DoD CIAO, and oversees DoD CIP program management.

Defense Threat Reduction Agency (DTRA)

The Defense Threat Reduction Agency (DTRA) safeguards the United States and its allies from weapons of mass destruction (chemical, biological, radiological, nuclear, and high-yield explosives) by reducing the present threat and preparing for future threats. Under DTRA, DoD resources, expertise, and capabilities are combined to ensure that the United States remains ready and able to address the present and future threat of weapons of mass destruction. DTRA's mission consists of four essential functions: combat support, technology development, threat control, and threat reduction. It greatly contributes to the CIP effort by conducting Balanced Survivability Assessments of DoD installations.

Joint Program Office - Special Technology Countermeasures (JPO-STC)

Since 1990, the Joint Program Office - Special Technology Countermeasures (JPO-STC), chartered by the Office of the Secretary of Defense to support the DoD's Infrastructure Assurance Program (IAP), has been working to assure DoD's mission-essential infrastructure. JPO-STC's mission is to support the Combatant Commanders,

the Military Services, and DoD mission planners by analyzing dependencies on supporting infrastructure, assessing impacts of infrastructure disruptions to DoD missions, and identifying mitigation options that strengthen DoD's operational posture.

Mission Assurance Operations Center (MAOC)

The Mission Assurance Operations Center (MAOC) was established in March 2001 to manage and integrate day-to-day support, mission taskings, and product development requested from the Joint Chiefs of Staff (JCS), the Combatant Commanders, the Services, and DoD organizations and installations. The MAOC broadens and strengthens the mission of the JPO-STC: it allows DoD planners to assess their infrastructure dependencies as well as the potential impact on military operations of the degradation or the disruption of key defense and commercial infrastructure components.

The Center supports peacetime, day-to-day management through the spectrum of conflict to crisis management and/or war. It operates in a war room-like environment, focusing on support in the following areas:

- Providing a physical location for integration and fusion of requirements
- Providing a product development crucible
- Organizing to allow rapid response to emergent tasking
- Operating, when necessary, on a 24-hour availability basis
- Providing a proactive—versus reactive—support environment
- Providing and leverage total JPO expertise and talent
- Directing the JPO toward operational capability and support

The MAOC's projected tactical, quick-response focus ensures appropriate task receipt and tracking, project monitoring, and effort prioritization, for effective customer support. The Agency allows for the rapid integration of broad expertise within the JPO analysis and assessment organization, enabling the organization to apply its full strength to mission tasking. The MAOC provides for the monitoring of the infrastructure assurance plans and policy at the national and DoD levels. This ensures strategic long-range planning by the JPO-STC to proactively anticipate organizational and leadership dynamics and develop customer requirements. This strategic approach provides the solid JPO-STC mission foundation on which to base task integration and management and product development.

Significant Accomplishments in CIP Organization since 9-11

Establishment of U.S. Northern Command (USNORTHCOM)

The Pentagon—November 20, 2001. Photo courtesy of Space Imaging.

October 1, 2002, saw the establishment of USNORTHCOM at Peterson Air Force Base in Colorado. USNORTHCOM's area of operations includes the United States, Canada, Mexico, parts of the Caribbean, and the contiguous waters in the Atlantic and Pacific oceans. The Command is responsible for land, aerospace, and sea defense of the United States and will command U.S. forces that operate within the United States in support of civil authorities. It will provide civil support not only in response to attacks but also in the event of natural disasters. As the operational Combatant Commander for homeland defense, USNORTHCOM will execute a leading role in critical infrastructure protection.

Department of the Navy Critical Infrastructure Protection Program

In order to maintain a global maritime presence and to have the ability of projecting military force worldwide, the U.S. Navy depends on critical assets and infrastructure, both domestic and overseas. To respond to potential threats against these critical infrastructures, the Department of the Navy (DON) has established actions to implement specific goals for an effective CIP program:

- Ensure the development of an integrated CIP capability
- Support the development of Sector Assurance Plans
- Integrate the efforts of other related DON programs into CIP
- Support the development of an integrated indications-and-warning capability
- Establish a web-based clearinghouse for DON CIP-specific information and guidance
- Establish long-term programmatic objectives for DON CIP

A particularly successful Navy program has been the development of an integrated analysis-and-assessment capability, the Naval Integrated Vulnerability Assessment (NIVA). This process allows the Navy to conduct comprehensive vulnerability assess-

ments of Navy ports and facilities in concert with commercial, information assurance, Defense Security Service, U.S. Coast Guard, Combatant Command, and other pertinent assessments.

Combatant Command Infrastructure Protection Programs

As of October 2002, all US combatant commands identified CIP as part of the top ten command initiatives and programs. This recognition came, in fact, as a result of exceptional work accomplished in Pacific Command, Joint Forces Command, and Central Command, laying the foundation for the Unified Commands on how best to manage CIP.

Pacific Command (USPACOM) - In September 2001, the Chairman of the Joint Chiefs of Staff designated USPACOM the lead supported Combatant Command, tasking it to develop a CIP Appendix 16 to a standing OPLAN. This appendix will serve as a template for other Combatant Commands. Appendix 16 will provide a framework for the identification of OPLAN Tier 1 assets and the determination of those assets to establish vulnerabilities and infrastructure interdependencies.

In January 2002, USPACOM hosted a CIP conference which established an exceptional forum for promoting CIP knowledge exchange and information sharing among the Combatant Commands. The original goal of the conference had been to further develop the CIP program within USPACOM. Because of DoD-wide interest in the topic of CIP, however, the conference grew to encompass Combatant Commands, sectors, Services, agencies, and other support functions. Action officers from the Commands had the opportunity to meet in order to discuss CIP implementation issues.

Before September 11, 2001, Pacific Command had already begun developing a dynamic CIP program. The Command was working to identify first- and second-tier assets, using this data to populate a usable CIP database, and defining Combatant Commanders' mission failure and degradation. Work was under way to develop a comprehensive USPACOM CIP instruction outlining policy, guidance, and responsibilities that would lead to a Theater Infrastructure Assurance Plan. Plans were made to integrate CIP into USPACOM exercises, which required educating headquarters staffs about CIP and led to the creation of an Asymmetric Threat Working Group. Defense Emergency Response Funds received in the wake of September 11 allowed USPACOM to accelerate its CIP Appendix 16 and database development efforts.

Central Command (USCENTCOM) - In August 2002, USCENTCOM initiated and hosted a Combatant Commanders' CIP conference. The purpose of the forum was to exchange information, ideas, and recommendations among Combatant Commands, Joint Staff, JPO-STC, and DTRA. The conference featured presentations concerning the Joint Staff support of Combatant Commands, Combatant Commands' role in CIP and Appendix 16 development, JPO-STC and DTRA CIP efforts, and budgeting for CIP. USPACOM discussed its Appendix 16 development and lessons learned with the group. The U.S. Joint Forces Command (USJFCOM) and Northern Command (USNORTHCOM) discussed their efforts to develop the Common Relevant Operational Picture (CROP). In all, the three-day conference provided the Combatant Commands with an opportunity to begin developing a unified approach to CIP.

The Combatant Commanders will follow up the August 2002 conference with a CIP conference held at USPACOM in January.

Joint Forces Command (USJFCOM) - Joint Force Headquarters Homeland Security (JFHQ-HLS) is the homeland security component of USJFCOM that coordinates the land and maritime defense of the continental United States on the one hand and military assistance to civil authorities on the other. JFHQ-HLS plans, integrates, and executes the full spectrum of civil support and homeland defense support to lead Federal agencies such as the Federal Emergency Management Agency (FEMA). Support includes prevention, crisis response, and consequence management.

In coordination with other Federal, state, and local agencies, JFHQ-HLS is constantly evaluating events and locations throughout the United States for their potential as terrorist targets. In addition, it provides information to military commands and civilian agencies to aid in their homeland security awareness and planning.

As the "transformation laboratory" of the U.S. military, USJFCOM has taken a leading role in DoD CIP concept development efforts. Two noteworthy examples of these initiatives are the Homeland Infrastructure Foundation Level Data (HIFLD) Working Group and Common Relevant Operational Picture (CROP).

Significant Technical Accomplishments since 9-11

Common Relevant Operational Picture (CROP)

USJFCOM has been experimenting with a revolutionary new system that will allow joint warfighters to interoperate in gathering vital information, communicating it to fighters in the field, and collaborating with joint leaders and strategists around the world.

Known as Common Relevant Operational Picture (CROP), this system is a presentation of timely, fused, accurate, and relevant information that can be tailored to meet the requirements of the joint force commander and the joint force and is common to every organization and individual involved in a joint operation. CROP gives the commander the relevant information required to make command decisions and to provide situational awareness in threat assessment, warning dissemination, and consequence response/ management.

With CROP, military thinkers, intergovernment agencies, and joint warfighting commanders are now able to review intelligence on their adversary, to chart and map troop movements, to gather information on an extensive database of knowledge and scenarios, and to get the information to the troops in a way never before used by any force in the world.

Through the use of a wide area network (WAN) linking personnel nationwide, this new system will be tested during Millennium Challenge 2002, the major joint integrating operation coordinated by USJFCOM that will incorporate elements of all Military Services, the U.S. Special Operations Command, the U.S. Transportation Command, the U.S. Space Command, and other DoD organizations and Federal agencies.

NIMA/USGS 133 Cities Mapping Project

The National Imagery and Mapping Agency (NIMA)/U.S. Geological Service (USGS) 133 Cities Project is a collaborative effort by Federal, state, and local government agencies and commercial firms to gather and maintain important geospatial data in support of homeland defense and emergency preparedness. This is an expansion of NIMA's 120-city requirement (which existed before 11 September 2001) for geospatial data covering cities identified as potential targets for terrorists. The USGS has been tasked with ensur-

ing the availability of imagery and geospatial data for the United States, as NIMA does not have this mission within the country. FEMA and NIMA therefore rely on the USGS for domestic geospatial data. The USGS provides remotely sensed imagery and basic cartographic information (transportation networks, coastlines and hydrography, significant cultural features, and vegetative cover) to help give emergency response teams and the U.S. military the ability to assist civilian agencies and the public in the event of a chemical, biological, radiological, nuclear, or high-yield explosive situations such as those recently experienced.

Vital CIP Partnerships

Not since World War II have commercial, government, defense, state, and local workers come together as they have in the projects supporting the DoD and National CIP efforts. In the last few months, the HIFLD and the NIMA/USGS efforts have become the hallmarks of cooperation. In an effort that would normally have taken decades, they have improved the flow of data and vital sensor information for defense and homeland infrastructure security.

Homeland Infrastructure Foundation Level Data (HIFLD) Working Group

The HILFD working group is best described as a loose coalition of Federal organizations, state agencies, supporting contractors, and Federally Funded Research and Development Centers (FFRDCs) that are concerned in some way with homeland security, critical infrastructure protection, and crisis and consequence management. This community of interest does not have a formal charter but works to promote information sharing and knowledge management among its members. Membership is based on participation, either in person at the monthly working sessions or through some form of communication indicating continuing interest.

The working group that was to evolve into HIFLD first met in February 2002 to identify data sets held by each organization, to determine data gaps within the HLS community, and to promote information sharing. To date, more than 100 individual agencies/organizations have participated in the working group. HIFLD is currently led by four organizations: the Joint Force Headquarters for Homeland Security, the Joint Program Office - Special Technology Countermeasures, the Joint Task Force for Civil Support, and the North America and Homeland Security Division of the National Imagery and Mapping Agency (NIMA).

Already, HIFLD has identified more than 400 foundation-level databases of interest to the national CIP community. The working group has made unprecedented progress in connecting Service and state geospatial information system (GIS) efforts with national GIS enterprises and has established previously nonexistent links between agencies and organizations working on similar or complementary projects. The synergy fueled by the HIFLD coalition has resulted in a steady and continuous increase in participation over the course of the monthly working group meetings.

Domestic Emergency Response Information Services (DERIS)

The Domestic Emergency Response Information Services (DERIS) project was funded following the events of September11 to demonstrate the ability of existing commercial off-the-shelf (COTS) technology and civilian telecommunication networks to support real-time information exchange and collaboration between first responder agencies and local, state and federal agencies.

DERIS was successfully demonstrated on 12 March 2002 through a DoD-sponsored exercise linking coordinated terrorist attack scenarios in Chicago, Los Angeles, and San Diego. Dozens of agencies shared resources, leads, and expertise in real time, via teleconferenced video, controlled access to critical applications, data and email. With this successful demonstration, DERIS has emerged as the most practical and quickest solution to the challenge of emergency communications and information access during natural and man-made disasters.

Using existing technology, DERIS created a common communications backbone into which different agencies may plug. Once logged into the DERIS Internet portal, they access resource information, collaborate, share information as it happens, and communicate with each other in real time, through video, voice, e-mail and other means. Critical to the success of DERIS was its ability to fit into the existing protocols of the emergency management community.

Taking CIP into the Future

Identification and Protection of Scenario-Independent Critical Infrastructure Assets

Scenario-independent critical infrastructure assets are required by multiple missions, Commands, DoD or other Federal agencies, and (in some cases) the private sector. Consequently, the disruption or failure of these assets would have an adverse impact on multiple missions, day-to-day operations, and perhaps on our national or economic security.

These defense-critical infrastructure assets are of great interest to the DoD leadership and, in some cases, to the national leadership. To make risk management decisions and to allocate resources for remediation and mitigation, it is essential to be quite aware of the interdependencies of these assets and the consequences of their degradation or loss.

In response to various queries from senior DoD leadership, the DoD CIP community has begun a near—term emphasis effort-of nearly two years—to support a macrolevel analysis, built on DoD Component data, of critical installations and facilities. Based on Combatant Commander missions and Defense-wide operational requirements, commercial and industrial infrastructures will be analyzed for an assessment of their impact on military- and infrastructure-sector operations and of their dependencies on these infrastructures. This effort will develop a better understanding of the interdependencies among various infrastructure assets. In addition, it will provide a basis for determining the efficiency and effectiveness of contingency plans to ensure mission success, even in the event of disruptions to key infrastructure components. This analysis will determine the operational impact of policies requiring the outsourcing of key defense infrastructures. The effort will also determine the impact of single points of failure and their impact on other industrial capabilities.

"The Government must make systematic security improvements to the nation's infrastructure . . . the CIA and law enforcement can't protect the U.S. against all threats."

CIA Director George Tenet,
28 June 2002

Mission Assurance Asset Database

Following the September 11, 2001 terrorist attacks, the C3I CIP Directorate and the Joint Staff Strategic Plans Office (J5) polled the DoD operational community for a list of critical (Tier 1) installations and facilities. This list has since matured into a functional database that allows to examine critical capabilities and vulnerabilities, as well as to prioritize critical sites by more than 100 possible asset combinations and query variations. The JPO - STC has been tasked with (1) maturing and improving the quality of the DoD's Critical Asset List Database—which is being developed as an operational support tool with DoD counterintelligence and criminal investigative elements to help focus assets—and (2) developing a priority listing to support ongoing and continuous Survivability Assessments. When these development efforts are complete, the Critical Asset List Database will serve as the solid foundation of a first-rate decision support tool.

Mission Degradation Analysis (MIDAS)

OASD(C3I) invited DTRA to participate in the DoD CIP Execution Plan by producing tools that allow to assess the impact of the degradation of critical infrastructures upon selected DoD missions and functions. In December 2000, DTRA established the Mission Degradation Analysis (MIDAS) program, which leverages DTRA's experience in managing technically challenging R&D contractual efforts relating to system protection and survivability. Assessing the degradation of critical infrastructures and its impact on DoD's missions and functions is a complex effort because of two factors: the scope of the mission and the complexity of infrastructure interdependencies.

The MIDAS program has the following objectives:

- Produce an automated tool set that integrates methodologies and models for assessing the effects of degradation of the critical infrastructures on selected DoD missions, using, when possible, existing infrastructure tools and models
- Apply these methodologies and models to CIPIS-approved mission evaluations to quantify the impact and consequences
- Assist in developing recommended tools for installation/organizational commanders to correct the effects of degradation of critical infrastructures on DoD's missions and to restore critical services

Who to Contact in the DoD CIP Directorate And JCS CIP Office

Mr. John P. Stenbit, Assistant Secretary of Defense (C3I),
DoD CIO, and DoD CIAO; 703-695-0348; john.stenbit@osd.mil

Ms. Carol A. Haave, Deputy Assistant Secretary of Defense (S&IO),
and Deputy DoD CIAO; 703-695-2396; carol.haave@osd.mil

OSD/C3I CIP Directorate

Mr. Tom Bozek, Director; 703-602-9973; tom.bozek@osd.mil
Mr. Mark Centra; 703-602-9984; mark.centra@osd.mil
Lt. Col. Lemoyne Blackshear; 703-602-9962; Lemoyne.blackshear@osd.mil
Mr. Eddie Craig; 703-602-5874; edward.craig@osd.mil
Mr. Jim Myers; 703-602-9972; jim.myers@osd.mil
Mr. Glenn Price; 703-602-9967; glenn.price@osd.mil
Lt. Col. Will Smith; 703-602-5676; wilburn.smith@osd.mil
Mr. Chuck Sadek, LNO - JPO-STC; 703-602-6997; chuck.sadek@osd.mil

Joint Staff (J-5 Homeland Security Division)

Col. David Barile, Division Chief; 703-679-1433; david.barile@js.pentagon.mil
Col. Bruce Beebe; 703-695-4955; bruce.beebe@js.pentagon.mil

Joint Program Office - Special Technology Countermeasures

Mr. John Keenan; 540-653-8730; keenanjp@nswc.navy.mil
Mr. Dan Mathis; 540-653-6454; mathised@nswc.navy.mil
Mr. Randy Sultzer; 540-653-2780; sultzerrt@nswc.navy.mil